CS60082 Computational Number Theory

Class Test 1

Maximum marks: 20 February 11, 2010 **Duration:** 1 hour

[*This test is open-notes. Answer all questions. Be brief and precise.*]

1 Let $a_1, a_2, \ldots, a_n$ be non-zero integers, and $d = \gcd(a_1, a_2, \ldots, a_n)$. Prove that there exist integers $u_1, u_2, \ldots, u_n$ with the property that $u_1a_1 + u_2a_2 + \cdots + u_na_n = d$. **(6)**

Solution First, note that $d = \gcd(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n)$. Now, proceed by induction on n. For $n = 2$, the result is the original Bézout relation. For $n \geqslant 3$, suppose that we have integers $v_1, v_2, \ldots, v_{n-1}$ with $\gcd(a_1, a_2, \ldots, a_{n-1}) = v_1a_1 + v_2a_2 + \cdots + v_{n-1}a_{n-1}$. By the original Bézout relation, we have $u \gcd(a_1, a_2, \ldots, a_{n-1}) + va_n = d$ for some $u, v \in \mathbb{Z}$. Now, take $u_i = uv_i$ for $i = 1, 2, \ldots, n-1$, and $u_n = v$.

2 Prove that the multivariate linear congruence $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$ is solvable for $x_1, x_2, \ldots, x_n$ if and only if $\gcd(a_1, a_2, \ldots, a_n, m) \mid b$. **(6)**

Solution Let $d = \gcd(a_1, a_2, \ldots, a_n, m)$. By Exercise 1, we have $u_1a_1 + u_2a_2 + \cdots + u_na_n + um = d$ for some $u_1, u_2, \ldots, u_n, u \in \mathbb{Z}$. Let $d \mid b$, that is, $b = kd$ for some $k \in \mathbb{Z}$. But then $a_1(ku_1) + a_2(ku_2) + \cdots + a_n(ku_n) \equiv b \pmod{m}$. Conversely, if the given congruence has a solution for $x_1, x_2, \ldots, x_n$, we have $a_1x_1 + a_2x_2 + \cdots + a_nx_n - lm = b$ for some $l \in \mathbb{Z}$. But then d divides the left side, and so the right side too.

3 Let p be a prime > 3. Prove that 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$. **(8)**

Solution By the law of quadratic reciprocity, $\left(\frac{3}{p}\right) = (-1)^{(3-1)(p-1)/4} \left(\frac{p}{3}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right)$. Therefore, $\left(\frac{3}{p}\right) = 1$ if and only if both the factors $(-1)^{(p-1)/2}$ and $\left(\frac{p}{3}\right)$ are $+1$, or both are -1, that is, either

(1) $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{3}$, or

(2) $p \equiv 3 \pmod{4}$ and $p \equiv 2 \pmod{3}$.